CLAIMS

1. A method of recording data to a recording medium, comprising steps of:

detecting, when a recorder is going to record data to the recording medium, whether a terminal unit with a memory having user identification information recorded therein is connected;

exchanging, when it is detected that the terminal unit is connected, an encryption key between the recorder and terminal unit;

encrypting the user identification information read from the memory with the exchanged encryption key and sending it from the terminal unit to the recorder; and

encrypting the data to be recorded to the recording medium with the user identification information sent from the terminal unit and recording the encrypted data to the recording medium.

2. The method according to claim 1, wherein:

when it is detected that the terminal unit is connected to the recorder, the recorder authenticates the terminal unit; and

when the recorder has not successfully authenticated the terminal unit, data recording to the recording medium is ceased.

3. The method according to claim 2, wherein when the recorder has not successfully authenticated the terminal unit, an error message is displayed.

4. The method according to claim 1, wherein when it is detected that the terminal unit is not connected to the recorder, a display is made to indicate that the

terminal unit is not connected.

5. The method according to claim 1, wherein the user identification information stored in the memory is set by the user.

6. The method according to claim 5, wherein the user identification information includes a user name.

7. The method according to claim 6, wherein the user identification information includes information unique to the terminal unit, having been set at the time of shipment from factory.

8. A playback method of decrypting encrypted data read from a recording medium, comprising steps of:

detecting, when a player is going to play back the recording medium having recorded therein user identification information intended to identify the user and data encrypted with the user identification information, whether a terminal unit with a memory having the user identification information recorded therein is connected to the player;

exchanging, when it is detected that the terminal unit is connected, an encryption key between the player and terminal unit;

encrypting the user identification information read from the memory with the exchanged encryption key and sending it from the terminal unit to the player;

judging whether the user identification information sent from the terminal unit is coincident with that read from the recording medium; and decrypting the encrypted data read from the recording medium when it is judged that the user identification information sent from the terminal unit is coincident with that read from the recording medium.

9. The method according to claim 8, wherein when it is judged that the user identification information sent from the terminal unit is not coincident with the user identification information read from the recording medium, it is inhibited to output data read from the recording medium.

10. The method according to claim 8, wherein:

when it is detected that the terminal unit is connected to the recorder, the recorder authenticates the terminal unit; and

when the recorder has not successfully authenticated the terminal unit, data recording to the recording medium is ceased.

11. The method according to claim 10, wherein when the recorder has not successfully authenticated the terminal unit, an error message is displayed.

12. The method according to claim 8, wherein when it is detected that the terminal unit is not connected to the recorder, a display is made to indicate that the terminal unit is not connected.

13. The method according to claim 8, wherein the user identification information stored in the memory is set by the user.

14. The method according to claim 13, wherein the user identification information includes a user name.

15. The method according to claim 14, wherein the user identification information includes information unique to the terminal unit, having been set at the time of shipment from factory.

16. A method of playing back a recording medium, comprising steps of:

judging, when a player is going to play back a recording medium having recorded therein data having buried therein user identification information intended to identify the user and which have been encrypted with the user identification information, whether user identification information read from an information holder provided in the player to hold user identification information sent from a terminal unit is coincident with user identification information read from the recording medium; and

decrypting the encrypted data read from the recording medium when the user identification information read from the information holder is coincident with that read from the recording medium.

17. The method according to claim 16, wherein:

when it is judged that the user identification information read from the information holder is not coincident with the user identification information read from the recording medium, it is detected whether the terminal is connected;

when the terminal unit is connected, it is judged whether the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium; and

when the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium, the data read from the recording medium is decrypted.

18. The method according to claim 16, wherein:

when the terminal unit is connected, an encryption key is exchanged between the player and terminal unit; and

the user identification information read from the memory is encrypted with the exchanged encryption key and sent from the terminal unit to the player.

19. The method according to claim 17, wherein when it is judged that the user identification information sent from the terminal unit is not coincident with the user identification information read from the recording medium, it is inhibited to output data read from the recording medium.

20. The method according to claim 17, wherein:

when it is detected that the terminal unit is connected to the player, the player authenticates the terminal unit;

when the terminal unit has not successfully been authenticated, it is inhibited to output data read from the recorder.

21. The method according to claim 20, wherein when the terminal unit has not successfully been authenticated, an error message is displayed.

22. The method according to claim 17, wherein when it is detected that the terminal unit is not connected to the recorder, a display is made to indicate that the terminal unit is not connected.

23. The method according to claim 17, wherein the user identification information stored in the memory is set by the user.

24. The method according to claim 23, wherein the user identification information includes a user name.

25. The method according to claim 24, wherein the user identification information includes information unique to the terminal unit, having been set at the time of shipment from factory.

26. A data transmitting method, wherein:

when an output unit to output data read from a recording medium having recorded therein data having buried therein user identification information intended to identify the user and which have been encrypted with the user identification information, is going to output data read from the recording medium, it is judged whether user identification information supplied from a terminal unit with a memory having the user identification information stored therein is coincident with that read from the recording medium;

when it is judged that the user identification information supplied from the terminal unit is coincident with that read from the recording medium the output unit sends, to a server, the user identification information showing the coincidence;

the server sends, to the output unit, a reference number based on the received user identification information; and

the output unit buries the received reference number into the data read from the recording medium and sends it to the server.

27. The method according to claim 26, wherein:

when it is judged that the user identification information supplied from the terminal unit is coincident with the user identification information read from the recording medium, an encryption key is exchanged between the output unit and server; and

the user identification information showing the coincidence is encrypted with the exchanged key and sent to the server.

28. The method according to claim 26, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the user identification information read from the recording medium, sending the data read from the recording medium is ceased.

29. The method according to claim 26, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the user identification information read from the recording medium, a display is made on a display unit of the output unit to prompt the user to select other data recorded in the recording medium.

30. The method according to claim 26, wherein the server stores data sent from the output unit into a storage unit provided in the server.

31. The method according to claim 26, comprising steps of:

detecting whether the terminal unit is connected;

judging, when the terminal unit is connected, whether the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium; and

decrypting the data read from the recording medium when the user identification information sent from the terminal unit is coincident with the user identification information read from the recording medium.

32. The method according to claim 31, wherein when the terminal unit is connected, an encryption key is exchanged between the output unit and terminal unit, and the user identification information read from the memory is encrypted with the exchanged encryption key and sent from the terminal unit to the output unit.

33. The method according to claim 31, wherein:

the output unit has an information holder to hold the user identification information sent from the terminal unit; and

when it is detected that the terminal unit is not connected, it is judged whether the user identification information read from the information holder is coincident with the user identification information read from the recording medium.

34. A method of controlling data recording, wherein:

there is sent, upon request for sending data stored in a storage unit provided in a server and which has stored therein a plurality of data having at least buried therein user identification information intended to identify the user and which have been encrypted with the user identification information, the requested data to a recorder;

the recorder extracts the user identification information from the received data;

it is judged whether the extracted user identification information is coincident with user identification information held in an information holder provided in the recorder; and

the recorder records the received data to the recording medium when the extracted user identification information is coincident with the user identification information held in the information holder in the recorder.

35. The method according to claim 34, wherein when it is judged that the extracted user identification information is not coincident with the user identification information held in the information holder in the player, it is judged whether user identification information in the received data is to be rewritten.

36. The method according to claim 35, wherein when it is judged that the user identification information in the received data is not to be rewritten, the received data is recorded to the recording medium.

37. The method according to claim 36, wherein when it is judged that the user identification information in the received data is to be rewritten, the recorder acquires the user identification information in the received data from the server, decrypts the received data, re-encrypts the decrypted data with new user identification information and records it to the recording medium.

38. The method according to claim 37, wherein when it is judged that the user identification information in the received data is to be rewritten, the new user

identification information is sent from the recorder to the server.

39. The method according to claim 37, wherein:

when it is judged that the user identification information in the received data is to be rewritten, the server judges whether the user identification information can be rewritten; and

when the user identification information can be rewritten, the recorder acquires the user identification information in the received data from the server.

40. The method according to claim 39, wherein the server judges, based on the solvency of a grantee of the data sent from the recorder, whether the user identification information can be rewritten.

41. The method according to claim 39, wherein when it is judged that the user identification information cannot be rewritten, the recorder records the received data to the recording medium.

42. The method according to claim 37, wherein user identification information is acquired from the received data;

the data is decrypted with the user identification information acquired from the data; and

when the data have not successfully been recorded to the recording medium, the recorder deletes the data having not successfully been recorded.

43. The method according to claim 41, wherein:

the data decrypted with the new user identification information is re-encrypted;

and

when the re-encrypted data have not successfully been recorded to the recording medium, the recorder sends a failure-in-storage signal to the server.

44. The method according to claim 37, wherein:

the data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted data have successfully been recorded to the recording medium, charging is made for the data thus recorded.

45. The method according to claim 43, wherein:

the data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted data have successfully been recorded to the recording medium, the recorder supplies the server with a success-in-storage signal and the charging is made based on the success-in-storage signal.

46. The method according to claim 37, wherein:

a reference signal is additionally buried in data to be stored into the storage unit; and

when it is judged that user identification information in the received data is to be rewritten, the recorder sends the reference signal to the server and the server will operate based on the received reference signal.

47. A data transmitting/receiving method, wherein:

it is judged, when a recorder/player outputs data read from a recording medium having recorded therein data having buried therein user identification information intended to identify the user and which have been encrypted with the user identification information, whether the user identification information supplied from a terminal unit with a memory having user identification information recorded therein is coincident with the user identification information read from the recording medium;

when it is judged that the user identification information supplied from the terminal unit is coincident with that read from the recording medium, the recorder/player sends, to a server, the user identification information showing the coincidence;

the server sends, to the recorder/player, a reference number based on the received user identification information;

the recorder/player buries the received reference number into the data read from the recording medium, sends it to the server and stores it into a storage unit provided in the server;

there is sent, upon request for sending data stored in the storage unit in the server, the requested data to the recorder/player;

the recorder/player extracts the user identification information from the received data;

it is judged whether the extracted identification information is coincident with that stored in the memory in the terminal unit; and the recorder/player records the received data to the recording medium when it is judged that the extracted user identification information is coincident with that stored in the memory.

48. The method according to claim 47, wherein when it is judged that the user identification information supplied from the terminal unit is not coincident with the user identification information read from the recording medium, sending the data read from the recording medium is ceased.

49. The method according to claim 47, wherein when it is judged that the extracted user identification information is not coincident with the user identification information stored in the memory, it is judged whether user identification information in the received data is to be rewritten.

50. The method according to claim 49, wherein when it is judged that the user identification information in the received data is not to be rewritten, the recorder/player records the received data to the recording medium.

51. The method according to claim 50, wherein when it is judged that the user identification information in the received data is to be rewritten, the recorder/player acquires user identification information in the data sent from the server, decrypts the data received from the server, re-encrypts the decrypted data with new user identification information and records the data to the recording medium.

52. The method according to claim 51, wherein:

when it is judged that the user identification information in the received data is to be rewritten, the server judges whether the user identification information can be rewritten; and

when the user identification information can be rewritten, the recorder/player acquires user identification information from the data sent from the server.

53. The method according to claim 52, wherein the server judges, based on the solvency of a grantee of the data sent from the recorder/player, whether the user identification information can be rewritten.

54. The method according to claim 53, wherein when it is judged that the user identification information cannot be rewritten, the recorder/player records the received data to the recording medium.

55. The method according to claim 51, wherein user identification information is acquired from the received data;

the data is decrypted with the user identification information acquired from the data;

the decrypted data is re-encrypted with new user identification information; and

when the data have not successfully been recorded to the recording medium, the recorder/player deletes the data having not successfully been recorded.

56. The method according to claim 55, wherein:

the data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted data have not successfully been recorded to the recording medium, the recorder/player sends a failure-in-storage signal to the server.

57. The method according to claim 51, wherein:

the data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted data have successfully been recorded to the recording medium, charging is made for the data thus recorded.

58. The method according to claim 57, wherein:

the data decrypted with the new user identification information is re-encrypted; and

when the re-encrypted data have successfully been recorded to the recording medium, the recorder supplies the server with a success-in-storage signal and the charging is made based on the success-in-storage signal.